Cyberattack on the Virginia Attorney General's Office: A Comprehensive Analysis (February 2025)

The cyberattack targeting the Virginia Attorney General's Office (AGO) in February 2025 represents a significant event in the ongoing landscape of cybersecurity threats against government entities. As the state's chief legal and prosecutorial agency, the AGO holds a substantial amount of sensitive information, the compromise of which could have far-reaching implications. This report aims to provide a comprehensive analysis of this incident, drawing upon available information to detail its chronology, technical aspects, impact, the official response, the involvement of investigative agencies, and the potential actors and motivations behind the attack. Understanding the intricacies of this event is crucial for appreciating the evolving challenges in cybersecurity and for developing effective strategies to mitigate future risks for similar organizations.

The initial signs of the cyberattack on the Virginia Attorney General's Office became apparent on **Wednesday, February 12, 2025**.[1] The attack was detected in the early morning, around **6:45 a.m.** [1], prompting immediate action from the agency. In response to the suspicious activity, officials made the decision to shut down the office's entire computer system as a precautionary measure to contain the potential breach.[2] Later that day, the severity of the situation was communicated to the AGO's approximately 700 employees through an email from Chief Deputy Attorney General Steven Popps. The email confirmed that a significant cyber incident had occurred, resulting in the shutdown of most of the office's information technology infrastructure.[1]

The disruption caused by the cyberattack was extensive, affecting a wide range of critical systems. According to reports, nearly all systems within the Attorney General's Office were rendered offline. This included essential tools and platforms such as Net Docs, a document management system; Outlook, the primary email client; Teams, a collaboration and communication platform; OAG Fileshare, likely an internal file-sharing service; and crucial network access points like VPN and internet connectivity via the AGO network.[3] Furthermore, the agency's website was also taken offline, limiting external communication and access to public resources.[2] The severity of the disruption necessitated a significant change in operational procedures, with employees being directed to revert to traditional paper-based methods for court filings. This instruction underscored the extent to which the agency's digital workflows had been compromised, forcing a return to less efficient, manual processes to maintain essential legal functions.[2]

The cyberattack on the Virginia Attorney General's Office was quickly characterized as "sophisticated" by the agency itself.[2] This initial assessment suggests that the attack involved advanced techniques designed to evade the existing security measures in place. Such sophistication often implies a targeted operation, executed by skilled actors with the resources and knowledge to penetrate robust cyber defenses, rather than a more opportunistic or less complex attempt.[5]

In a significant development that shed more light on the nature of the attack, the ransomware group known as **Cloak** claimed responsibility for the incident in March 2025.[6] This claim was made public when the group added the Virginia AGO to their Tor-based leak site on **March 20, 2025**.[6] This action

by ransomware groups typically follows a failure to extort the targeted organization, indicating that the Attorney General's Office likely did not meet the ransom demands, if any were made.[6] Alongside their claim of responsibility, Cloak allegedly made data stolen from the AGO's systems available for download on their leak site, claiming to have exfiltrated a substantial **134GB** of data.[8] This suggests a potential double extortion tactic, where the attackers aim to profit both by encrypting data and threatening to release sensitive information publicly if their demands are not met.

Further analysis of the Cloak ransomware group reveals it to be a ransomware-as-a-service (RaaS) operation that first emerged in late 2022.[6] The group employs an **ARCrypter variant** for its encryption process, which is reportedly derived from the leaked source code of the Babuk ransomware.[6] There is also a belief within the cybersecurity community that Cloak has ties to the Good Day ransomware group, as both operations have been observed sharing a common data leak platform.[6] Cloak's primary methods for gaining initial access to target networks include the use of sophisticated social engineering techniques, such as phishing campaigns, and collaborations with initial access brokers (IABs) who specialize in breaching networks and selling that access to ransomware operators.[6] Historically, Cloak has predominantly focused on targeting small- and medium-sized businesses (SMBs) located in Europe and Asia. The attack on the Virginia AGO marks their first confirmed incident targeting a U.S. entity in 2025, indicating a potential shift or expansion in their operational scope.[6]

Technically, the Cloak ransomware exhibits several advanced capabilities. **It is known to terminate processes associated with antivirus software, backup solutions, and database services, hindering the victim's ability to recover and increasing the likelihood of ransom payment**.[7] The malware also deletes volume shadow copies, which are often used for system restoration, and empties the recycle bin, further complicating recovery efforts.[7] Cloak employs both full and intermittent encryption strategies based on file size, utilizing the HC-128 encryption algorithm.[7] To evade detection and ensure persistence within the compromised system, Cloak has been observed running from virtual hard disks and modifying registry entries to enable automatic startup.[7] It also employs techniques such as enabling SeDebugPrivilege, respawning itself, and terminating debugging or profiling tools to further enhance its stealth and resilience.[7] These technical details paint a picture of a highly capable and evasive ransomware operation.

The cyberattack had a significant impact on the operational capabilities of the Virginia Attorney General's Office. The disruption of essential services such as email, VPN access, and internet connectivity severely hampered the ability of attorneys and staff to conduct their daily tasks.[2] These systems are critical for communication, accessing legal databases, conducting research, and managing case files. The shutdown of internal services and applications further compounded the issue, affecting various aspects of the agency's workflow.[6] Perhaps the most indicative measure of the attack's severity was the directive for employees to revert to paper-based processes for court filings.[2] This return to manual methods, in an era heavily reliant on digital systems, likely resulted in substantial delays, increased administrative burdens, and reduced efficiency in the agency's core legal functions. The inability to access digital case files and electronic communication platforms

would have created significant challenges in managing ongoing litigation and providing timely legal services.

The claim by the Cloak ransomware group of exfiltrating 134GB of data raises serious concerns about the potential compromise of sensitive information held by the Attorney General's Office.[8] State attorneys general, including Virginia's, handle a wide array of sensitive data, including legal briefs containing confidential arguments and strategies, detailed case files with potentially privileged information, and investigative data related to ongoing law enforcement actions.[2] Furthermore, the Attorney General's Office provides legal services to a broad spectrum of state entities, including agencies, boards, commissions, colleges, and universities.[3] This expansive role means that the types of data potentially at risk could be diverse and highly sensitive. State attorneys general also collect and manage data related to crime statistics, consumer debt, and other sensitive areas.[2] The potential exposure of such a large volume of information could lead to severe consequences, including breaches of confidentiality, legal and regulatory ramifications, and significant reputational damage for the Attorney General's Office and the Commonwealth of Virginia.

The official response from the Virginia Attorney General's Office in the immediate aftermath of the cyberattack was characterized by internal communication but a lack of public disclosure. As noted earlier, Chief Deputy Attorney General Steven Popps sent an email to employees on the evening of the attack, informing them of the incident and the widespread system outages.[2] This internal notification was crucial for keeping the agency's workforce informed about the situation and providing guidance on how to proceed with their work despite the significant challenges.[2] However, the Attorney General's Office did not immediately release any public statements detailing the cyberattack or its impact.[6] Moreover, the Office of Attorney General Jason Miyares did not respond to requests for comment from various news outlets seeking information about the incident.[2] This initial silence in the public sphere could be attributed to several factors. It is common practice for organizations dealing with active cyber incidents to limit public communication to avoid compromising ongoing investigations or providing potentially useful information to the attackers. Additionally, there might have been strategic considerations related to the nature of the attack, particularly if it was suspected to be a ransomware incident, where public acknowledgment might be avoided in the early stages.

Following the detection of the cyberattack, the Virginia Attorney General's Office promptly notified relevant law enforcement and state technology agencies.[2] The Virginia State Police, the Federal Bureau of Investigation (FBI), and the Virginia Information Technologies Agency (VITA) were all informed of the suspicious activity that led to the system shutdowns.[2] Subsequently, both the Virginia State Police and the FBI initiated investigations into the incident.[2] The involvement of these law enforcement agencies underscores the seriousness of the cyberattack and the potential for significant legal and security ramifications. The Virginia State Police, as the primary state law enforcement agency, would likely be involved due to the attack targeting a key state government office. The FBI's participation suggests the possibility of a federal nexus, the need for specialized cybercrime investigation expertise, or the potential involvement of interstate or international actors.

VITA, the state's central IT agency, declined to comment on the incident, citing the ongoing investigation.[2] VITA's role would likely involve providing technical assistance to the Attorney General's Office in assessing the damage, understanding the attack vectors, and supporting the recovery and remediation efforts. The coordinated involvement of these agencies highlights the multi-faceted approach required to respond to and investigate significant cyber incidents targeting government infrastructure.

Since the initial reports of the cyberattack in February 2025, the most significant update has been the claim of responsibility by the Cloak ransomware group in March 2025.[6] As previously mentioned, Cloak added the Virginia AGO to their leak site and claimed to have exfiltrated a substantial amount of data.[6] This public acknowledgment by the ransomware group provides a crucial piece of information regarding the likely nature of the attack and the potential threat actor involved.[6] However, beyond this claim, there has been a notable lack of official statements or further updates from the Virginia Attorney General's Office or the investigating law enforcement agencies.[7] This continued silence from official sources could indicate that the investigation is still in progress and involves sensitive aspects that cannot be publicly disclosed at this time.[7] It might also reflect a deliberate strategy to avoid further communication with the ransomware group or to limit the information available to potential adversaries. Without official updates, the claim by Cloak remains the most recent publicly available information regarding the status of the investigation.

Based on the available information, the likely perpetrator behind the cyberattack on the Virginia Attorney General's Office is the Cloak ransomware group.[6] Their public claim of responsibility, coupled with the technical characteristics of the attack aligning with their known tactics, techniques, and procedures (TTPs), strongly suggests their involvement.[6]

The primary motivation behind ransomware attacks, including those attributed to the Cloak group, is typically **financial gain through extortion**.[6] These groups encrypt a victim's data and demand a ransom payment, usually in cryptocurrency, in exchange for the decryption key.[10] In many cases, including this one, there is also a potential for **double extortion**, where the attackers exfiltrate sensitive data and threaten to release it publicly if the ransom is not paid for data decryption.[7] The posting of allegedly stolen data from the Virginia AGO on Cloak's leak site supports this possibility.[8] While the initial reports following the attack in February did not mention any ransom demand [2], the subsequent actions of the Cloak group indicate that a demand was likely made privately and not met, leading to the public data leak.[7] While financial gain appears to be the primary driver, other potential motives, such as disrupting government operations or accessing sensitive legal information for other malicious purposes, cannot be entirely ruled out, although these are less common for ransomware groups primarily focused on monetary rewards.[11] The specific reasons why the Virginia Attorney General's Office was targeted by Cloak remain unknown, but it is plausible that the perceived value of the data held by the agency or its potential willingness to pay a ransom made it an attractive target.

Examining previous cyberattacks on government entities can provide valuable context and potential lessons learned for the incident involving the Virginia Attorney General's Office. Two notable cases

include the ransomware attack on the Hampton Roads Sanitation District (HRSD) in November 2020 and the attack on the Illinois Attorney General's Office in April 2021.

The HRSD attack involved **Ryuk ransomware** and began with an initial entry point through a malicious Excel spreadsheet containing **ZLoader malware**.[12] The systems affected included Windows business systems, email, and billing infrastructure.[13] Attackers also utilized Cobalt Strike for command and control within the HRSD network.[13] This incident resulted in significant disruption to billing and customer service operations.[14] Notably, wastewater treatment services remained operational throughout the attack.[15] HRSD engaged cybersecurity experts, and the investigation into the attack was ongoing for some time.[15] The organization reportedly recovered from the attack in approximately three weeks.[12]

In April 2021, the Illinois Attorney General's Office was targeted by a ransomware attack involving **DoppelPaymer malware**.[16] This attack led to the theft and subsequent publication of agency files, including sensitive personal information.[17] Similar to the Virginia AGO attack, the Illinois incident disrupted lawyers' access to essential work-related products and research.[17] The cost of recovery for the Illinois AGO was substantial, exceeding $2.5 million, and involved engaging various cybersecurity firms for assistance.[18] A prior audit had identified weak cybersecurity practices within the Illinois AGO.[16] While no ransom was paid, the office invested significantly in rebuilding its systems and enhancing its overall security posture.[18]

These comparative analyses highlight several key points. Both the Virginia AGO and the Illinois AGO attacks targeted similar legal institutions and resulted in significant disruptions to their IT infrastructure. Both incidents also involved the exfiltration of sensitive data, leading to concerns about potential data breaches. The HRSD attack, while on a different type of critical infrastructure, also demonstrates the potential for ransomware to disrupt essential services, although in that case, the core operational technology remained secure. The recovery timeline for HRSD (around three weeks) might offer a potential timeframe for the Virginia AGO's recovery, although the specifics of each attack and the preparedness of the organization can significantly influence this. The substantial cost of recovery for the Illinois AGO underscores the financial implications of such cyber incidents. Furthermore, the prior finding of weak cybersecurity practices in the Illinois case emphasizes the importance of proactive security measures and regular audits to identify and address vulnerabilities before an attack occurs.

Technical Details of Cloak Ransomware	
First Appearance	Late 2022
Type	Ransomware-as-a-Service (RaaS)
Encryption Algorithm	ARCrypter variant (Babuk code), HC-128
Initial Access Vectors	Social Engineering, Initial Access Brokers (IABs)
Target Focus	SMBs in Europe & Asia, expanded to US
Evasion Techniques	Runs from VHDs, modifies registry, enables SeDebugPrivilege, respawns, terminates debugging tools
Persistence Mechanisms	Modifies registry for startup
Disruption Tactics	Terminates security & backup processes, deletes shadow copies
Extortion Tactics	Encryption, Data Exfiltration, Leak Site
Reported Payment Rate	91-96%

In conclusion, the cyberattack on the Virginia Attorney General's Office in February 2025 represents a serious security incident with significant operational and potential data compromise implications. The likely involvement of the sophisticated Cloak ransomware group underscores the persistent and evolving threat posed by such actors to government entities. The attack caused widespread disruption to the AGO's IT systems, forcing a return to manual processes and raising concerns about the confidentiality and integrity of sensitive legal and personal data. The prompt notification of law enforcement agencies, including the Virginia State Police and the FBI, indicates the gravity of the situation and the ongoing efforts to investigate the incident. The claim by Cloak of data exfiltration in March 2025 provides a crucial update, suggesting a failed ransom attempt and highlighting the double extortion tactics commonly employed by ransomware operators.

This incident serves as a critical reminder of the importance of robust cybersecurity measures for government organizations. Proactive threat detection, the development and regular testing of comprehensive incident response plans, and ongoing employee training to recognize and avoid social engineering attacks are essential components of a strong security posture. Furthermore, transparency and effective communication, balanced with the need to protect sensitive information and the integrity of investigations, are crucial for maintaining public trust and managing the aftermath of a cyberattack. Legal institutions, in particular, face unique challenges due to the sensitive nature of the information they handle, necessitating a thorough and continuous review of their cybersecurity protocols and infrastructure. Drawing lessons from this incident and comparable attacks, such as those on HRSD and the Illinois AGO, is vital for identifying vulnerabilities, enhancing security measures, and developing effective recovery strategies. Organizations should also establish clear policies regarding ransomware demands and ensure these are well-understood across the agency. Finally, fostering collaboration and information sharing between government agencies, law enforcement, and cybersecurity experts is paramount in the collective effort to address the ever-increasing cyber threat landscape and protect critical infrastructure and sensitive data.

Works cited

1. Virginia Attorney General's Office Hit by Cyber Attack, accessed April 29, 2025, https://www.insurancejournal.com/news/east/2025/02/14/812081.htm
2. 'Sophisticated' cyberattack downs systems at Virginia attorney general's office | StateScoop, accessed April 29, 2025, https://statescoop.com/cyberattack-virginia-attorney-general-office-2025/
3. Virginia Attorney General's office struck by cyberattack targeting attorneys' computer systems | AP News, accessed April 29, 2025, https://apnews.com/article/attorney-general-jason-miyares-cyberattack-0cf74a899064a72d4532fb0c38f8e382
4. Virginia AG's Office Struck by Cyberattack - Cville Right Now, accessed April 29, 2025, https://cvillerightnow.com/news/208802-virginia-ags-office-struck-by-cyberattack/
5. Virginia Attorney General's Office Reports Cyber Breach - The National CIO Review, accessed April 29, 2025, https://nationalcioreview.com/articles-insights/information-security/virginia-attorney-generals-office-reports-cyber-breach/
6. Ransomware Group Claims Attack on Virginia Attorney General's Office - SecurityWeek, accessed April 29, 2025, https://www.securityweek.com/ransomware-group-claims-attack-on-virginia-attorney-generals-office/
7. Cloak Ransomware Claims Attack on Virginia Attorney General's Office - Halcyon, accessed April 29, 2025, https://www.halcyon.ai/blog/cloak-ransomware-claims-attack-on-virginia-attorney-generals-office
8. Cloak Ransomware Attacks Virginia Attorney General's Office - Thailand Computer Emergency Response Team (ThaiCERT), accessed April 29, 2025, https://www.thaicert.or.th/en/2025/03/25/cloak-ransomware-attacks-virginia-attorney-generals-office/
9. Cyberattack Disrupts Virginia Attorney General's Office - MSSP Alert, accessed April 29, 2025, https://www.msspalert.com/brief/cyberattack-disrupts-virginia-attorney-generals-office
10. The State of Ransomware 2025 - BlackFog, accessed April 29, 2025, https://www.blackfog.com/the-state-of-ransomware-2025/
11. Top 7 Cyber Attacks in the United States - SentinelOne, accessed April 29, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-attacks-in-the-united-states/
12. The Ransomware Files, Episode 3: Critical Infrastructure, accessed April 29, 2025, https://www.bankinfosecurity.com/interviews/ransomware-files-episode-3-critical-infrastructure-i-4993
13. des.sc.gov, accessed April 29, 2025, https://des.sc.gov/sites/scdph/files/media/document/BOW_Cybersecurity_HRSDRoundTableDiscussion.pdf
14. HRSD, HRUBS Bill Payment Due Dates for November & December Bills Extended to Jan 31 without Penalty - City of Norfolk, accessed April 29, 2025, https://www.norfolk.gov/CivicAlerts.asp?AID=5269&ARC=10298
15. News Release - November 19, 2020 | HRSD, accessed April 29, 2025, https://www.hrsd.com/news-release-november-19-2020
16. Illinois attorney general acknowledges ransomware attack ..., accessed April 29, 2025,

https://statescoop.com/illinois-attorney-general-acknowledges-ransomware-attack/
17. Illinois attorney general's office victimised in ransomware attack | NZ ..., accessed April 29, 2025, https://www.thelawyermag.com/nz/news/general/illinois-attorney-generals-office-victimised-in-ransomware-attack/254488
18. No Ransom Paid, but Illinois AG Office Is Spending More Than $2.5 ..., accessed April 29, 2025, https://illinoisanswers.org/2021/07/29/no-ransom-paid-but-illinois-ag-office-is-spending-more-than-2-5-million-on-hacker-attack/
19. Attorney General - Illinois Leaks |, accessed April 29, 2025, https://edgarcountywatchdogs.com/category/illinois/attorney-general-illinois/